

CLAIMS

We Claim:

1. In a computer system comprising a processor and a memory, a method for detecting viruses in macros, the method comprising:
 2. obtaining comparison data including information for detecting a virus;
 3. retrieving a macro;
 4. decoding the macro to produce a decoded macro; and
 5. scanning the decoded macro for a virus by comparing the decoded macro to
the comparison data.

2. The method of claim 1, further comprising:
 1. removing the virus from the macro to produce a treated macro if the step of scanning the decoded macro indicates that the macro is infected with the virus.

3. The method of claim 1, wherein the step of retrieving a macro comprises:
 1. accessing a targeted file;
 2. determining whether the targeted file is a template file;
 3. if the targeted file is not a template file, determining whether the targeted file includes an embedded macro; and
 4. if the targeted file includes an embedded macro, locating the embedded macro.

4. The method of claim 1, wherein the comparison data includes a first suspect instruction identifier and a second suspect instruction identifier

1 5. The method of claim 4, wherein the step of scanning the decoded macro to
2 determine whether it includes a virus comprises:
3 determining whether the decoded macro includes a first portion which
4 corresponds to the first suspect instruction identifier;
5 determining whether the decoded macro includes a second portion which
6 corresponds to the second suspect instruction identifier; and
7 determining that the decoded macro includes the virus if the decoded macro
8 includes the first and second portions.

~~1 6. The method of claim 5, wherein the first suspect instruction identifier
2 detects a macro virus enablement instruction.~~

~~1 7. The method of claim 6, wherein the second suspect instruction identifier
2 detects a macro virus reproduction instruction.~~

~~1 8. The method of claim 7, wherein the step of removing the virus comprises:
2 locating a first suspect macro instruction in the decoded macro which
3 corresponds to the first suspect instruction identifier; and
4 removing the first suspect macro instruction.~~

~~1 9. The method of claim 8, further comprising:
2 verifying the integrity of the treated macro; and
3 replacing the infected macro in a targeted file with the ^{treated} ~~repaired~~ macro
4 dependent upon the integrity verification of the treated macro.~~

10. The method of claim 5, wherein the step of removing the first suspect macro instruction includes replacing the first suspect instruction with a benign instruction.

11. The method of claim 8, wherein the step of removing the virus comprises:
2 locating a second suspect macro instruction in the decoded macro which
3 corresponds to the second suspect instruction identifier; and
4 removing the second suspect macro instruction from the decoded macro to
5 produce a treated macro.

12. The method of claim 1, wherein the comparison data includes a plurality of
2 sets of suspect instruction identifiers.

13. The method of claim 12, wherein a first set of suspect instruction identifiers
comprises the strings 73 CB 00 0C 6C 01 00 and 67 C2 80.

14. The method of claim 13, wherein a second set of suspect instruction
identifiers comprises the strings 73 CB 00 0C 6C 01 00 and 64 6F 02 67 DE 00 73
3 87 01 12 73 7F, a third set of suspect instruction identifiers comprises the strings
4 73 CB 00 0C 6C 01 00 and 6D 61 63 72 6F 73 76 08, a fourth set of suspect
5 instruction identifiers comprises the strings 12 6C 01 00 and 64 67 C2 80 6A 0F
6 47, and a fifth set of suspect instruction identifiers comprises the strings 79 7C 66
7 6F 72 6D 61 74 20 63 6A and 80 05 6A 07 43 4F 4D.

15. In a computer system comprising a processor and a memory, a method for
detecting viruses in macros, the method comprising:
3 retrieving a macro;

4 obtaining comparison data for detecting a virus, the comparison data
5 including a first suspect instruction identifier and a second suspect
6 instruction identifier;
7 scanning the macro to determine whether the macro includes a first portion
8 which corresponds to the first suspect instruction identifier;
9 scanning the macro to determine whether the macro includes a second
10 portion which corresponds to the second suspect instruction
11 identifier; and
12 determining that the macro is infected with the virus if the macro includes
13 the first and second portions.

13
1 16. The method of claim 15, further comprising:
2 treating the macro to produce a treated macro if it is determined that the
3 macro includes the first and second portions.

14
1 17. The method of claim 16, wherein the step of treating the macro comprises:
2 locating a first macro instruction in the infected macro which corresponds
3 to the first suspect instruction identifier; and
4 removing the first macro instruction from the infected macro to repair the
5 infected macro.

15
1 18. The method of claim 17, wherein the step of treating the macro comprises:
2 locating a second macro instruction in the infected macro which
3 corresponds to the second suspect instruction identifier; and
4 removing the second macro instruction from the infected macro to repair
5 the infected macro.

1 16
1 19. The method of claim 15, wherein the step of retrieving a macro comprises:
2 accessing a targeted file; and
3 determining whether the targeted file is a template file;
4 if the file is not a template file, determining whether the targeted file
5 includes an embedded macro; and
6 if the file includes an embedded macro, locating the embedded macro.

1 20. The method of claim 15, wherein the first instruction identifier includes the
2 string 73 CB 00 0C 6C 01 00 and the second suspect instruction identifier
3 includes the string 67 C2 80.

1 17. 12
1 21. The method of claim 15, wherein the comparison data includes a plurality
2 of sets of suspect instruction identifiers.

1 22. The method of claim 21, wherein a first set of suspect instruction identifiers
2 comprises the strings 73 CB 00 0C 6C 01 00 and 67 C2 80, a second set of suspect
3 instruction comprises the strings 73 CB 00 0C 6C 01 00 and 64 6F 02 67 DE 00 73
4 87 01 12 73 7F, a third set of suspect instruction identifiers comprises the strings
5 73 CB 00 0C 6C 01 00 and 6D 61 63 72 6F 73 76 08, a fourth set of suspect
6 instruction identifiers comprises the strings 12 6C 01 00 and 64 67 C2 80 6A 0F
7 47, and a fifth set of suspect instruction identifiers comprises the strings 79 7C 66
8 6F 72 6D 61 74 20 63 6A and 80 05 6A 07 43 4F 4D.

1 23. The method of claim 15, further comprising:
2 accessing a targeted file; and
3 locating the macro within the targeted file;
4 removing the macro from the targeted file; and

5 adding the treated macro to the targeted file to produce a corrected file.

1 24. An apparatus for detecting viruses in macros, the apparatus comprising:
2 a virus information module, for storing comparison data for detecting a
3 virus, the comparison data including a first suspect instruction
4 identifier and a second suspect instruction identifier; and
5 a macro virus scanning module, in communication with the virus
6 information module, for receiving the comparison data and scanning
7 a macro to determine whether the macro includes a first portion
8 which corresponds to the first suspect instruction identifier and a
9 second portion which corresponds to the second suspect instruction
10 identifier.

1 25. The apparatus of claim 24, further comprising:
2 a macro locating and decoding module, in communication with the macro
3 virus scanning module, for accessing a targeted file, determining
4 whether the targeted file is a template file, determining whether the
5 targeted file includes an embedded macro, and decoding the macro
6 to produce a decoded macro.

1 26. The apparatus of claim 25, further comprising:
2 a macro treating module, in communication with the virus information
3 module, for accessing the decoded macro and removing a first macro
4 instruction which corresponds to the first suspect instruction
5 identifier and a second macro instruction which corresponds to the
6 second suspect instruction identifier to produce a treated macro.

1 27. The apparatus of claim 26, further comprising:
2 a file correcting module, in communication with the macro treating module,
3 for accessing the targeted file, locating the macro within the targeted
4 file, removing the macro from the targeted file and adding the treated
5 macro to the targeted file to produce a corrected file.

sub B
1 28. The apparatus of claim 27, wherein the first instruction identifier includes
2 the string 73 CB 00 0C 6C 01 00 and the second suspect instruction identifier
3 includes the string 67 C2 80.

1 29. The apparatus of claim 27, wherein the comparison data includes a plurality
2 of sets of suspect instruction identifiers.

1 30. The apparatus of claim 29, wherein a first set of suspect instruction
2 identifiers comprises the strings 73 CB 00 0C 6C 01 00 and 67 C2 80, a second set
3 of suspect instruction comprises the strings 73 CB 00 0C 6C 01 00 and 64 6F 02
4 67 DE 00 73 87 01 12 73 7F, a third set of suspect instruction identifiers comprises
5 the strings 73 CB 00 0C 6C 01 00 and 6D 61 63 72 6F 73 76 08, a fourth set of
6 suspect instruction identifiers comprises the strings 12 6C 01 00 and 64 67 C2 80
7 6A 0F 47, and a fifth set of suspect instruction identifiers comprises the strings 79
8 7C 66 6F 72 6D 61 74 20 63 6A and 80 05 6A 07 43 4F 4D.

1 31. An apparatus for detecting viruses in macros, the apparatus comprising:
2 means for obtaining comparison data for detecting a virus, the comparison
3 data including a first suspect instruction identifier and a second
4 suspect instruction identifier;

5 means for scanning the macro to determine whether a macro includes a first
6 portion which corresponds to the first suspect instruction identifier;
7 means for scanning the macro to determine whether the macro includes a
8 second portion which corresponds to the second suspect instruction
9 identifier; and
10 means for determining that the macro is infected with the virus if the macro
11 includes the first and second portions.

1 ²⁵ ²⁴ 32. The apparatus of claim 31, further comprising:
2 means for locating a first macro instruction and a second macro instruction
3 within the macro which respectively correspond to the first suspect
4 instruction identifier and the second suspect instruction identifier;
5 and
6 means for removing the first macro instruction and the second macro
7 instruction from the macro to produce a treated macro.

1 33. The apparatus of claim 32, further comprising:
2 means for accessing a targeted file and determining whether the targeted
3 file includes a macro.

1 34. The apparatus of claim 33, further comprising:
2 means for correcting a file, the means for correcting a file including means
3 for accessing the targeted file, means for removing the macro from
4 the targeted file and means for adding the treated macro to the
5 targeted file to produce a corrected file.

1 35. A system for detecting viruses in macros, the system comprising:

2 a memory, for storing routines and comparison data for detecting a virus,
3 the comparison including a first suspect instruction identifier and a
4 second suspect instruction identifier; and
5 a processor, in communication with the memory, for receiving the
6 comparison data and scanning a macro to determine whether the
7 macro includes a first portion which corresponds to the first suspect
8 instruction identifier and a second portion which corresponds to the
9 second suspect instruction identifier.